

JANUARY 2025

Comprehensive Web Protection: Leveraging AWS WAF and Partner Solutions

John Grady, Principal Analyst

Abstract: Changing applications architectures create more distributed applications reliant on APIs and open additional attack vectors. This has made it harder to achieve comprehensive visibility and maintain protection. Through its broad technical partner ecosystem, AWS provides customers with the flexibility to use partner-built tools for advanced use cases like observability and API protection, without the integration overhead and complexity that is typically required.

Protecting Web Applications Remains a Significant Challenge for Many

As digital transformation has accelerated, web applications have become more critical than ever to help businesses engage and transact with customers. At the same time, cloud infrastructure, agile development methodologies, and cloud-native application architectures have all increased the speed with which applications can be deployed, leading to significant growth in many organizations' application footprint. In fact, research from Informa TechTarget's Enterprise Strategy Group found that 69% of organizations support at least 100 public facing web applications and websites.¹

Yet while this increase in speed and scale can help the business differentiate and drive revenue, the security implications of these shifts are significant. Specifically, 55% of organizations said securing their web applications has become more difficult than it was two years ago. Of even more concern, 93% said their organization has experienced at least one attack on their web applications and APIs in the last 12 months. This is likely to grow further as attackers leverage generative AI to improve the scale and effectiveness of their attacks and as generative AI applications themselves impact corporate websites and applications. Yet even today, the attacks organizations face are varied (see Figure 1):

55% of organizations said securing their web applications has become more difficult, and 93% said their organization has experienced at least one attack on their web applications and APIs.

- **Traditional application attacks.** Attackers continue to use traditional avenues to compromise applications, leveraging malware and exploiting OWASP Top-10 vulnerabilities as well as lesser-known and zero-day vulnerabilities. Additionally, various denial-of-service attacks target application availability, creating business impacts even if sensitive data is not put at risk.
- **API attacks.** As cloud-native architectures have taken hold, and applications have become more interconnected by APIs, attackers have shifted their focus to these endpoints. Similar to direct attacks on the

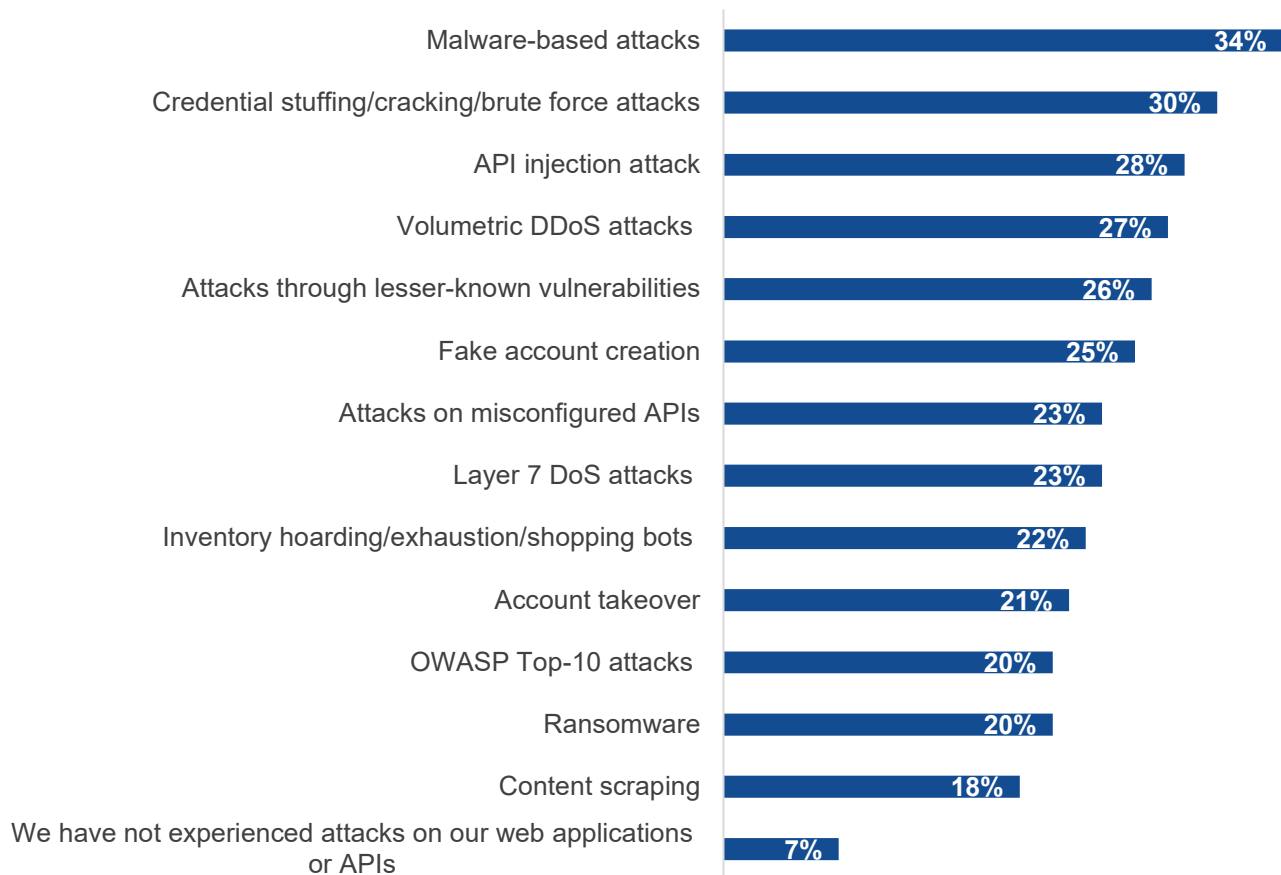
¹ Source: Enterprise Strategy Group Research Report, [Trends in Modern Application Protection](#), July 2022. All Enterprise Strategy Group research references and charts in this showcase are from this report.

application itself, APIs can be targeted with injection attacks (such as SQL and cross-site scripting), as well as exploitation of misconfigured endpoints (such as weak or default passwords or other authentication issues).

- Bot and fraud attacks.** In both cases, attackers often use bots to scale their attacks and make detection more difficult. In many of these attacks, the end goal is account fraud, which can be achieved by credential stuffing and cracking, fake account creation, and account takeover. But other actions such as inventory hoarding and content scraping can create negative effects as well. While this data is from 2022, the impact of generative AI has only grown in the time since. AI bot scraping is one example of an emerging issue many security teams are beginning to struggle with. As the prevalence and scale of generative AI apps continue to grow, the impact on web traffic and applications will only increase as they crawl corporate websites and applications.

Figure 1. Most Common Types of Web Application Attacks

Which of the following types of web application and API attacks has your organization experienced over the last 12 months? (Percent of respondents, N=366, multiple responses accepted)



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

A Strong WAF Should Be the Foundation, But Security Teams Need Simplicity, Broad Capabilities, and Flexibility

The fact that so many organizations cited challenges protecting their web applications and are experiencing attacks is not due to a lack of web application security tools. In fact, most organizations use multiple tools to protect their web applications: Web application firewalls (WAFs) have been a staple for years, providing core protections against application attacks. Distributed denial of service (DDoS) prevention helps maintain application availability in the face of abusive traffic, API security is an emerging area to defend the endpoints that connect modern applications, and

bot mitigation and detection helps manage or block malicious automated traffic targeting application and APIs. Yet even with all these options, many continue to struggle with the very tools designed to protect them. Many of these issues can be grouped into challenges with efficiency and efficacy (see Figure 2).

On the efficiency front, correctly deploying, configuring, tuning, and managing these tools can be difficult, especially for the many organizations challenged by the cybersecurity skills shortage. Further, many attacks are now multivector, making it especially important for tools to be properly integrated to share telemetry and work in concert. Providing unified visibility supported by strong analytics is a particular challenge for many organizations. With many security teams struggling to keep pace as it is, when this process is manual, it introduces additional strain on the organization.

From an efficacy perspective, many web application security tools fail to accurately detect threats and help analysts quickly diagnose incidents. Tools that are noisy or generate too many false positives could be redeployed in alert rather than block mode, raising the chance that malicious activity gets through. Even alerts that can be legitimate offer limited value if they cannot provide analysts with valuable context. This could include the severity of the alert, the potential origin, the history of activity from that origin, whether other resources might have been impacted, and so on. In this way, the limited visibility many organizations struggle with affects both efficiency (as previously noted), as well as efficacy.

Figure 2. Top Challenges With Web Application Protection Tools



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

So where does this leave application security teams, and what’s needed for them to be in the best possible position to succeed? One trend that seeks to address these issues has been the convergence of many of the capabilities across application protection, API security, DDoS protection, and bot mitigation into a unified solution. Yet, while many WAFs today provide some capabilities in these areas, they might not meet the requirements of every security

team. Some organizations still prefer or require purpose-built bot or API security tools because they provide functionality above and beyond that which is available from a WAF. This makes it important to prioritize solutions that provide broad capabilities themselves, as well as the flexibility to use other tools to augment security and do both simply and effectively. This helps promote the efficiency and effectiveness that so many organizations say is missing from their current web application security approach.

AWS WAF: Strong Protection, Enhanced by Partners

AWS WAF is a web application firewall that helps protect web applications from attacks through rules that allow, block, or monitor web requests based on pre-defined conditions including IP addresses, HTTP headers, HTTP body, uniform resource identifier (URI) strings, and more. It is tightly integrated with other AWS application and website delivery services from Amazon, including Amazon CloudFront, the Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync. When used with these services, AWS WAF protection is distributed across all AWS edge locations, blocking malicious requests before they reach web servers and helping to ensure strong performance.

AWS WAF offers Managed Rules as an easy way to deploy preconfigured rules to protect applications from threats, including OWASP Top-10 vulnerabilities, bots, or Common Vulnerabilities and Exposures (CVE). AWS Managed Rules are available from both AWS (Managed rules for AWS WAF) and from third-party sellers (Managed Rules from AWS Marketplace) and can be used together in the same web policy rule set. Managed Rules can easily be subscribed to from the AWS WAF console or from the AWS Marketplace. Other key capabilities of AWS WAF include:

- **Web traffic filtering.** AWS WAF lets security teams create rules that filter web traffic based on conditions, including IP addresses, HTTP headers and body, or custom URIs. This adds an additional layer of protection from web attacks that attempt to exploit vulnerabilities in custom or third-party web applications. In addition, AWS WAF makes it easy to create rules that block common web exploits like SQL injection and cross-site scripting.
- **Bot control.** AWS WAF Bot Control is a Managed Rule group that provides visibility and control over bot traffic that can consume excess resources, skew metrics, cause downtime, or perform other undesired activities. Security teams can granularly block or rate-limit pervasive bots, such as scrapers, scanners, and crawlers, and can allow common bots, such as status monitors and search engines. The Bot Control Managed Rule group can be used alongside other Managed Rules for WAF or custom WAF rules to protect applications. It also addresses generative AI scraping.
- **Fraud prevention.** AWS WAF Fraud Control - Account Takeover Prevention is a Managed Rule group that monitors an application's login page for unauthorized access to user accounts using compromised credentials. The rule group can be used to help protect against credential stuffing attacks, brute force login attempts, and other anomalous login activities. JavaScript, iOS/Android, and AppleTV/AndroidTV SDKs are available to collect additional telemetry on user devices that attempt to log in to an application, which better protects against automated login attempts by bots. Similarly, Account Creation Fraud Prevention is a Managed Rule group that monitors an application's sign-up or registration page for creation of fake or fraudulent accounts. The rule group can be used to protect against abuse such as promotional or sign-up abuse, loyalty or rewards abuse, and phishing.
- **Centralized policy management.** Through integrations with AWS Firewall Manager, AWS WAF deployments can be centrally configured and managed across multiple AWS accounts. As new resources are created, common security rules can be applied, ensuring consistency. Firewall Manager automatically audits and informs security teams when there is a policy violation so that they can respond immediately and take action.

The AWS WAF Partner Ecosystem

While these capabilities are all critical to help security teams protect their web applications, what sets AWS WAF apart is its additional technology partnerships. These provide customers with the flexibility to use additional, best-in-class partner solution offerings to enhance security based on their use case. AWS WAF Ready partner offerings provide managed WAF rule sets and tools that customers can simply add to their AWS WAF deployment. The tight integration between AWS WAF and partner solutions promotes ease of use and supports centralized management so the customer feels as if they are using first-party services.

AWS WAF Ready partners provide customers with prebuilt integrations to help ingest and analyze WAF event data more efficiently. Customers can quickly identify validated AWS Partner software products vetted by AWS Partner Solutions Architects for their architecture, adherence to AWS best practices, and demonstrated customer success. Some of the key areas AWS WAF partners focus on include:

- **APIs.** API endpoints are an attractive target for attackers specifically because so many organizations lack specific security tools and often do not know the full scope of APIs in their environment. Partner solutions can help customers discover all the APIs in use at their organization, test for vulnerabilities and sensitive data exposure, and block malicious activity against those APIs.
- **Managed services.** Even with offerings such as Managed Rules, many organizations need additional help because they do not have the staff in place to manage application security tools. Partners that help automate the deployment, configuration, and management of AWS WAF by managed services can help security teams overcome this issue and, ultimately, achieve better security results.
- **Observability.** Even with all these tools in place, the fact that attackers will often exploit multiple threat vectors and target different parts of the application makes it critical to tie disparate pieces of telemetry together to create an accurate picture for security teams. Solutions from technology partners that aggregate this level of observability across web applications and provide an added analytics layer above the WAF can help security teams better identify anomalous behavior from bots, find fraudulent account activity, and detect data exfiltration.
- **Advanced Bot Detection.** While AWS WAF offers its own integrated bot control, AWS also works with ecosystem partners to offer customers advanced bot protection. Organizations that face high volumes of sophisticated or targeted bot traffic need more tailored solutions that provide broader and more sophisticated bot detection techniques, enhanced analytics and reporting, more granular customization and rule enforcement, and specialized support for specialized bot-related use cases.

Conclusion

Between the changes to application environments, the threat landscape, and security tools themselves, security teams have a lot to contend with when it comes to application security. They must strike a balance between promoted efficiency and ease of use, while also maintaining strong security to address disparate use cases. AWS supports this balance through the native security capabilities of its own WAF, coupled with a robust partner ecosystem to provide customers the flexibility to easily incorporate partner solutions to augment their application security strategy however they see fit.

AWS Partner Spotlight: Cequence Security

Cequence Security specializes in API security and bot management, protecting the applications and APIs that organizations depend on from attacks, business logic abuse, and fraud. Its unique Unified API Protection platform unites discovery, compliance, and protection capabilities, providing real-time security in the face of sophisticated threats. Demonstrating value in minutes rather than days or weeks, Cequence offers a flexible deployment model that requires no app instrumentation or modification. Cequence solutions scale to meet the demands of the largest and most demanding private and public sector organizations, protecting more than 8 billion daily API interactions and 3 billion user accounts.

For more information on Cequence Security, click [HERE](#).

Note: Content in the above Partner Spotlight section was provided by Cequence Security and edited for clarity by Enterprise Strategy Group. Enterprise Strategy Group has not necessarily been briefed by the featured partner and readers should perform their own research into the partner's offerings and capabilities.

©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for BrightTALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.


Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com

 www.esg-global.com